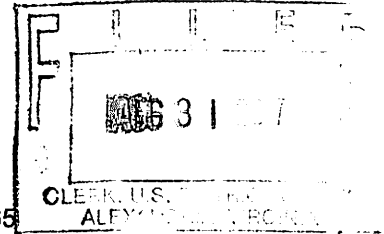


## UNITED STATES DISTRICT COURT

for the  
Eastern District of VirginiaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)4621 Luxberry Drive  
Fairfax, VA 22032

Case No. 1:17-SW-565



## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

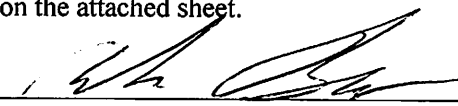
Code Section	Offense Description
21 U.S.C. § 844	Possession of Controlled Substance
18 U.S.C. § 922(g)(3)	Unlawful possession of a firearm by a controlled substance user
18 U.S.C. §§1341, 1349	Honest services mail fraud and Conspiracy

The application is based on these facts:  
See attached affidavit

- ☐ Continued on the attached sheet.  
☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Samantha Bateman and Kimberly Pedersen

  
Applicant's signature

SA Andrew Berger, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/31/2017
/s/ JFA  
John F. Anderson  
United States Magistrate Judge

Judge's signature

City and state: Alexandria, VA

John F. Anderson, U.S. Magistrate Judge

Printed name and title

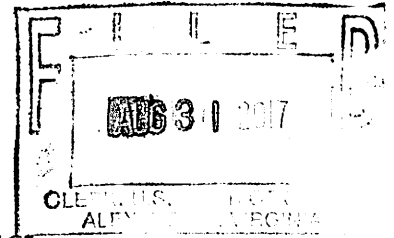
IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF SEARCH OF  
4621 LUXBERRY DRIVE  
FAIRFAX, VIRGINIA 22032

)  
)  
)  
)  
)

CASE NO. 1:17-SW-565



**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

Your affiant, Andrew Berger, being first duly sworn, states that the following is true to the best of his knowledge and belief:

**I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed for approximately 14 months. I am currently assigned to the Washington, D.C., Field Office, Northern Virginia Resident Agency, located in Manassas, Virginia. My principal duties include the investigation of white collar crime, including bribery and other public corruption offenses. I have received training in and have experience in the enforcement of the laws of the United States, including the preparation and presentation of search warrants, and in executing court-ordered search warrants. I have had training and experience in investigating and have worked with other FBI agents who have such experience, and who have provided me with additional information about such crimes.

2. I submit this Affidavit in support of an application by the United States for the issuance of a search warrant to search the premises located at 4621 Luxberry Drive, Fairfax, Virginia 22032 (hereinafter "the Target Residence"), as more further described in Attachment A to this Affidavit. More specifically, I submit that there is probable cause to believe that a

resident of 4621 Luxberry Drive, Fairfax, Virginia 22032, Shane Sariri, has committed violations of 18 U.S.C. § 922(g)(3) (possession of a firearm by an unlawful user of a controlled substance), 21 U.S.C. § 844 (possession of a controlled substance), and 18 U.S.C. §§ 1341 and 1349 (honest services mail fraud and conspiracy to commit honest services mail fraud), and that evidence, fruits, and/or instrumentalities of those crimes, including the items and records listed in Attachment B to this Affidavit, are currently present within the Target Residence to be searched.

3. The facts and information contained in this Affidavit are based upon my personal knowledge and the investigation and observations of other officers and agents involved in the investigation. All observations referenced below that were not personally made by me were related to me by the persons who made such observations. This Affidavit is intended to contain information necessary to support probable cause for this search warrant application. It is not intended to include each and every fact and matter observed by me or known to the Government.

## **II. FACTS IN SUPPORT OF PROBABLE CAUSE**

4. Since approximately early 2015, the FBI has been investigating allegations of bribery and public corruption involving schemes by Virginia Department of Transportation (VDOT) employees, including employees at the VDOT Burke Area Headquarters (AHQ), located within the Eastern District of Virginia, to solicit and accept bribe payments in exchange for, among other things, awarding snow removal work to private VDOT contractors during the winter snow seasons, signing off on VDOT invoices seeking payments for such snow removal work from VDOT, and conducting inspections and approving vehicles and other equipment for use in snow removal work on behalf of VDOT.

5. On or about August 24, 2017, a grand jury sitting in the Eastern District of Virginia returned a 40-count indictment charging two employees of the VDOT Burke AHQ

(Anthony “Andy” Willie (“Willie”), the Superintendent of Maintenance at the VDOT Burke AHQ, and Kenneth “Kenny” Duane Adams (“Adams”), the VDOT Burke AHQ Supervisor of Maintenance), as well as four snow removal contractors who have each performed snow removal work, such as snow plowing and sand and salt spreading operations, on behalf of the VDOT Burke AHQ, with numerous counts of honest services mail and/or wire fraud and conspiracy to commit the same.<sup>1</sup> The contractors charged in the indictment included Shaheen (“Shane”) Sariri (“Sariri”), who resides at 4621 Luxberry Drive, Fairfax, Virginia 22032, within the Eastern District of Virginia (hereinafter “the Target Residence”). Sariri was charged in the indictment with one count of conspiracy to commit honest services mail fraud, in violation of 18 U.S.C. § 1349, and nine substantive counts of honest services mail fraud, in violation of 18 U.S.C. § 1341, and a warrant was issued for his arrest by United States Magistrate Judge Ivan D. Davis.

6. On or about the morning of August 31, 2017, a team of FBI agents arrested Sariri on the above-described arrest warrant at the Target Residence, where Sariri was known to reside. The arresting agents included myself and six other agents of the FBI, along with one Fairfax County Police officer.

7. The arrest team arrived at the Target Residence at approximately 6:00 a.m. and knocked and announced the presence of law enforcement agents at the front door. Within approximately one minute, Sariri opened the front door. At that time, Sariri was clad only in a t-shirt and gym shorts, and was not wearing shoes. Sariri was placed under arrest while standing on the front porch of the Target Residence, directly outside the residence. However, in order to

---

<sup>1</sup> The indictment was originally returned under seal pending the arrests of all charged defendants, but all defendants were arrested on the morning of August 31, 2017, and the indictment and all related materials (*e.g.*, arrest warrants) have thus been unsealed at this time.

transport him for booking and further proceedings, it was necessary to allow him to re-enter the Target Residence briefly to put on footwear.

8. In connection with arresting Sariri, law enforcement agents asked him whether anyone else was present in the Target Residence, and Sariri answered in the negative. Sariri was also asked whether there were any weapons at the Target Residence, and he answered in the affirmative and disclosed that he possessed at least one firearm, which he described as an AR-15, in the Target Residence. As a result, the arrest team determined that it was necessary to perform a protective sweep of all rooms in the Target Residence to secure the scene and any weapons, ascertain that no other individuals were in fact present in the Target Residence, and ensure the safety of the arresting agents before accompanying Sariri into the Target Residence in order to allow him to put on footwear.

9. Six FBI agents performed the protective sweep of the Target Residence, while I, as the lead arresting agent, remained outside on the front porch with Sariri. The protective sweep lasted approximately two to three minutes. During the protective sweep of the Target Residence, the AR-15 weapon described by Sariri was not located, and no other weapons or persons were found. After the protective sweep was concluded, Sariri was escorted into the kitchen of the Target Residence and was seated at the kitchen table. Sariri then directed FBI agents to locate his shoes in the front hallway and he was permitted to put on his shoes before being transported by agents for booking.

10. While entering the Target Residence to perform the protective sweep, an FBI agent with experience investigating drug offenses smelled an odor consistent with marijuana. In addition, while performing the protective sweep of the Target Residence, FBI agents observed a glass table in the basement of the Target Residence with approximately six glass mason jars

containing a green leafy substance that, based on their training, experience, and observations, the agents noted was consistent with the appearance of marijuana. A small amount of the same green leafy substance was also loose on the glass table. Handwritten notes were also observed inside several of the glass jars, and one appeared to say "King Kush." A portable digital scale was also observed on the glass table, within inches of the glass jars, and a smoking device, commonly known as a bong, was observed on the ground within approximately one or two feet of the glass table. Based on my training and experience and conversations with other law enforcement personnel who have experience investigating and prosecuting violations of controlled substances laws, I am aware that scales are commonly associated with the distribution of controlled substances, and bongs are commonly associated with the consumption of controlled substances, including marijuana.

11. In addition, at the kitchen table where Sariri was seated while putting on his shoes, FBI agents observed two Virginia license plates with plastic packaging on the kitchen table, along with multiple brown file folders that were stacked on top of one another and appeared to contain documents, and an Apple laptop computer. The Apple computer was adjacent to the file folders, within approximately one foot of the folders.

12. Based on my participation in the bribery and public corruption investigation that gave rise to Sariri's arrest, I know that Sariri operated at least two snow removal companies, AMZ, Inc. ("AMZ") and AMSC, Inc. ("AMSC"), both of which were registered in the names of nominee owners but which Sariri used to provide snow removal work on behalf of the VDOT Burke AHQ and to pay bribes to Willie and Adams in exchange for snow removal work and approval of VDOT invoices.

13. For example, on or about February 24, 2016, FBI agents conducting surveillance observed Sariri entering the VDOT Burke AHQ. A confidential human source (hereinafter referred to as "CHS1") recorded Sariri speaking with Willie at that time about signing invoices to submit to VDOT seeking payment for alleged snow removal work. During the recording of the February 24, 2016 meeting, Willie can be heard directing Sariri to date the documents he is signing with a date of February 23, 2016, despite actually signing them on February 24, 2016. In addition, based on a review of the invoices submitted to VDOT, the FBI's investigation determined that invoices purportedly dated February 23, 2016 were in fact submitted to VDOT on behalf of AMZ and AMSC, seeking payments from VDOT in the amounts of \$82,249.25 and \$77,030.50, respectively. The AMZ invoice was purportedly signed by A.A., the nominal owner of that company, and the AMSC invoice was purportedly signed by S.S., Sariri's brother and the nominal owner of that company. However, based on the recording of the meeting and the FBI's surveillance of the VDOT Burke AHQ when the invoices were signed on or about February 24, 2016, during which no individual other than Sariri himself was observed entering the VDOT Burke AHQ, it appears that Sariri forged the signatures of A.A. and S.S. on behalf of AMZ and AMSC, respectively.

14. Also on or about February 24, 2016, CHS1 recorded an in-person meeting between Sariri, Willie, and Adams at an Outback Steakhouse in Fairfax, Virginia, within the Eastern District of Virginia. During that meeting, Willie was recorded discussing a bribery arrangement with Sariri, and he can be heard on the recording asking Sariri: "Now tell me if I'm wrong, you know, we agreed, each contract ten percent right, yeah?" Sariri can be heard responding on that same recording, in part: "The agreement's the agreement. That's what we

gonna stick by.” Sariri also says later during that same recording: “I want to steer away from leaving any sort of like paper trail.”

15. In addition, on or about March 18, 2016, FBI agents conducted surveillance at the same Outback Steakhouse in Fairfax, Virginia where the February 24, 2016 recorded meeting took place. During the March 18, 2016 surveillance, FBI agents observed Sariri, Willie, and Adams having lunch together and talking. The March 18, 2016 meeting was not recorded, but after the meeting, CHS1 told the FBI agents that Sariri had paid \$14,000 in cash to Willie and Adams at the Outback Steakhouse as part of their ongoing bribe arrangement in exchange for being awarded snow removal work on behalf of the VDOT Burke AHQ, and CHS1 surrendered his half of that cash bribe (*i.e.*, \$7,000) to the FBI.

16. The FBI’s investigation also uncovered evidence of bribes paid by Sariri to Willie and Adams in exchange for physical inspections of snow removal equipment and vehicles used by his nominee-owned companies, and their certifying such vehicles and equipment as having passed those inspections, and therefore as eligible for use in snow removal services on behalf of VDOT. For example, CHS1 disclosed to the FBI that on or about November 23, 2015, Sariri met Willie and Adams at the VDOT Burke AHQ and paid them \$500 each in exchange for their inspection of 15 vehicles that belonged to one of Sariri’s nominee-owned companies, and their certification of such vehicles as having passed those inspections. On or about November 24, 2015, at the FBI’s direction, CHS1 made a recorded call to Sariri during which he thanked him for the November 23, 2015 payment. On the recording on the November 24, 2015 call, Sariri can be heard to respond: “Absolutely, absolutely. I know all about it man. I know all about capitalism. Believe me.”



17. Based on my training and experience and my knowledge of the bribery and public corruption investigation that gave rise to Sariri's arrest, I know that VDOT employees and contractors who perform snow removal work on behalf of VDOT frequently maintain records of their business dealings, such as VDOT invoices and license and registration information relating to snow removal vehicles, drivers, and equipment at their residences. For example, during a search executed by the FBI on or about November 5, 2014 at the residence of CHS1, one of the VDOT employees at the Burke AHQ, pursuant to a search warrant issued by United States Magistrate Judge Theresa C. Buchanan, law enforcement agents located numerous VDOT invoices and handwritten notes relating to various VDOT contractors and apparent bribe payments from those contractors. At least one of the handwritten notes found during the search of CHS1's residence referenced one of Sariri's nominee-owned companies, AMSC.

18. In addition, while Sariri was being booked at the FBI's Washington Field Office after his arrest, Sariri stated that he was self-employed and worked from home. Based on those statements and the presence of the Virginia license plates, file folders, and Apple computer on the kitchen table in the Target Residence, I submit there is probable cause to believe that Sariri operates his nominee-owned snow removal companies, AMZ and AMSC, out of the Target Residence and that records relating to those companies, including possible evidence, fruits, and instrumentalities of bribe payments that were corruptly made to Willie, Adams, and/or other VDOT officials using those companies, or in exchange for snow removal work awarded to those companies, will be located at the Target Residence.

19. In addition, based on my training and experience, as well as my knowledge of the facts of this investigation, I know individuals who engage in financial frauds, including bribery and other public corruption schemes, often keep notes, records, and ledgers showing the amount

of money they and their businesses have received as well as notes, records, and other documents and items which reveal how bribes were paid and how money was dispersed, such as: bank records, deposit slips, records of money transfers, safe deposit box records and keys, and records of the purchase of expensive items. Based on my training and experience, as well as the information I have obtained during the course of this investigation, I have found that such business and financial records may be saved in hard copy form, or electronically stored on computer systems or maintained with computer hardware equipment and software, such as disks, magnetic tapes, programs, and computer printouts.

20. Based on my training and experience, as well as the information I have obtained during the course of this investigation, I am aware of some of the techniques and methods used by individuals and businesses involved in illegal activity, including bribery schemes. I have found that businesses frequently keep records of illegal bribes and other payments, but often disguise them as legitimate transactions to eliminate drawing attention to the businesses and their criminal activities. I have further found violators employ many tactics to conceal illegal payments, including but not limited to the alteration and falsification of records. It has been my experience that financial records of a business entity or enterprise are usually kept and maintained at the entity's business office and/or home office if the proprietor operates the business out of residence. These records include such things as: general journals, cash receipts journals, cash disbursement journals, and sales journals; general and subsidiary ledgers, accounts receivable, accounts payable and closing ledgers; bank statements, deposit slips and canceled checks for any and all bank accounts; receipts and invoices for all expenditures; federal income tax and employment tax returns; and addresses and telephone numbers of business associates and other persons and entities. All such records may also be kept and maintained in hard copy form,

or electronically stored on computer systems or maintained with computer hardware equipment and software, such as disks, magnetic tapes, programs, and computer printouts.

21. Since the execution of the arrest warrant for Sariri at approximately 6:00 a.m. on the morning of August 31, 2017, and continuing through the present time, the Target Residence has been secured by agents of the FBI and other law enforcement agencies. Accordingly, the Target Residence and all items and potential evidence contained within the Target Residence have been maintained in the same condition as when they were observed by law enforcement agents pursuant to the arrest of Sariri and the protective sweep of the Target Residence.

### **III. PROCEDURES FOR SEARCHING ELECTRONIC DEVICES**

22. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. Digital devices, including mobile devices, may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,”

erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword

terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices do not store data as searchable text; rather, the data is saved in a proprietary non-text format. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers

the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

23. Based on all of the foregoing, I believe that searching any electronic devices, such as the Apple laptop computer, located within the Target Residence pursuant to the applied-for warrant may require a wide array of electronic data analysis techniques and may take significant time to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices.

24. In light of these difficulties, I request permission to seize any electronic devices located at the Target Residence which could contain any of the items or evidence listed in Attachment B to this Affidavit and transport them to law enforcement personnel who are trained in computer forensics and/or the extraction of electronic data from electronic devices, who may then use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of the applied-for warrant from said devices. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas


to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

25. In searching the seized electronic storage media or digital devices, forensic examiners may examine as much of the contents of the devices as is deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized electronic storage media or digital devices will be specifically chosen to identify only the specific items to be seized under the applied-for warrant.


#### IV. CONCLUSION

26. Based on the information provided in this Affidavit, I respectfully submit that probable cause exists that evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 922(g)(3) (possession of a firearm by an unlawful user of a controlled substance), 21 U.S.C. § 844 (possession of a controlled substance), and 18 U.S.C. §§ 1341 and 1349 (honest services mail fraud and conspiracy to commit honest services mail fraud), are currently present at the premises of 4621 Luxberry Drive, Fairfax, Virginia 22032 ("the Target Residence"), as described in Attachment A.

27. In consideration of the foregoing, your affiant respectfully requests that this Court issue a warrant to search the premises of 4621 Luxberry Drive, Fairfax, Virginia 22032, as described in Attachment A, for the items listed in Attachment B.

  
Special Agent Andrew Berger  
Federal Bureau of Investigation

Sworn to and subscribed before me on this 31<sup>st</sup> day of August, 2017.

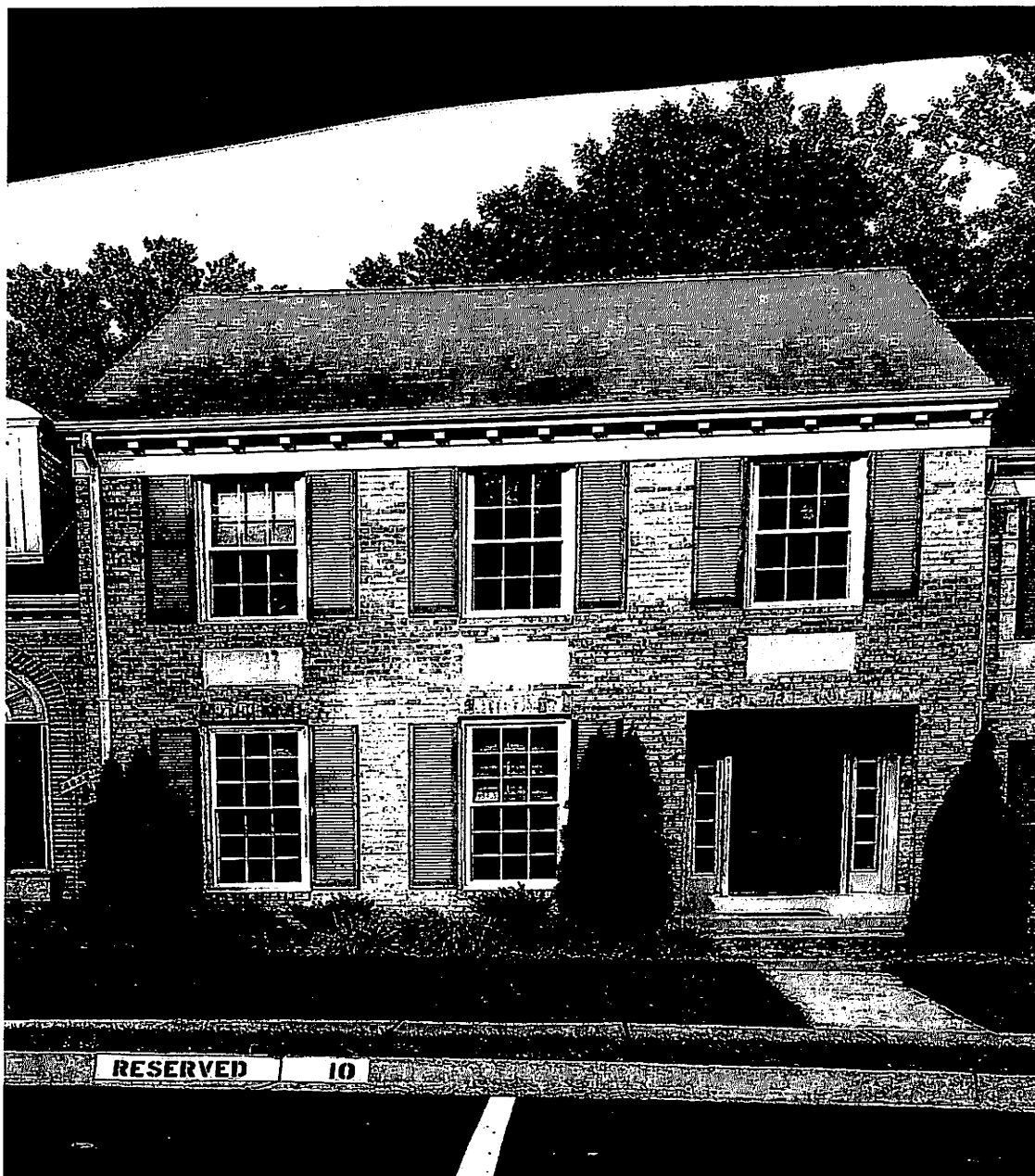
  
\_\_\_\_\_/s/\_\_\_\_\_  
John F. Anderson  
United States Magistrate Judge  
Honorable John F. Anderson  
United States Magistrate Judge



**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

The Target Residence to be searched is the residence of Shaheen “Shane” Sariri, a two-story tan brick building with a below-ground basement, a light brown roof, a dark brown front door, and brown shutters on the windows, located at 4621 Luxberry Drive, Fairfax, Virginia, 22032. A photograph of the front of the residence is below:



**ATTACHMENT B**

**ITEMS TO BE SEIZED**

Any fruits, evidence, and/or instrumentalities of violations of 18 U.S.C. § 922(g)(3), 21 U.S.C. § 844, and 18 U.S.C. §§ 1341 and 1349, including the following:

1. United States currency and financial instruments, including but not limited to money orders, cashier's checks, and personal checks;
2. Firearms, including but not limited to an AR-15 style firearm, and firearms ammunition;
3. Controlled substances, including but not limited to marijuana, and controlled substances paraphernalia, including but not limited to scales and smoking devices commonly known as bongs;
4. Any and all records and documents reflecting the purchase and/or sale of controlled substances, and names, addresses and contact information for suppliers and/or customers of controlled substances;
5. Any and all records and documents evidencing the purchase and ownership of firearms, including but not limited to an AR-15 style firearm;
6. All financial documents and records, whether in hard copy or electronic format, relating to Shane Sariri, AMZ, Inc., AMSC, Inc., Kenneth Adams, Anthony Willie, and the Virginia Department of Transportation (VDOT), including VDOT invoices, checks, and other payments or records of payments, bank records, cashier's checks, safe deposit keys, statements of accounts, returned and/or canceled checks, checkbooks and stubs, duplicates and copies of checks, checkbook registers, deposit items, savings passbooks, ATM receipts, ATM cards, check cards, credit cards and bank envelopes, and handwritten notes;
7. All receipts or records of purchases, whether in hard copy or electronic format, made by or for Shane Sariri, AMZ, Inc., AMSC, Inc., Kenneth Adams, Anthony Willie, and/or VDOT;
8. All records of vehicle registrations, licenses and license plates, titles and other documents reflecting ownership of vehicles and snow removal equipment, and inspections of vehicles and snow removal equipment, whether in hard copy or electronic format, made by or for Shane Sariri, AMZ, Inc., AMSC, Inc., Kenneth Adams, Anthony Willie, and/or VDOT;
9. All calendars, appointment books, and other papers or records, whether in hard copy or electronic format, reflecting appointments with and/or names, addresses and/or telephone numbers of Shane Sariri, Kenneth Adams, Anthony Willie, AMZ, Inc.,

and AMSC, Inc., and/or officers, directors, or employees of those companies, and/or employees of VDOT;

10. All records and documents, whether in hard copy or electronic format, indicating communications between and among Shane Sariri, Kenny Adams, and Anthony Willie, AMZ, Inc., and AMSC, Inc., and/or officers, directors, or employees of those companies, and/or employees of VDOT; and

11. Any electronic devices, including an Apple laptop computer and any mobile devices, and any locked or closed containers which could contain any of the above-listed evidence.